UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/520,274	01/18/2005	Eli Yanovsky	29238	9022

67801 7590 08/04/2009

MARTIN D. MOYNIHAN d/b/a PRTSI, INC.
P.O. BOX 16446
ARLINGTON, VA 22215

EXAMINER	
KANAAN, SIMON P	
ART UNIT	PAPER NUMBER
2432	
MAIL DATE	DELIVERY MODE
08/04/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/520,274	YANOVSKY, ELI	
	Examiner	Art Unit	
	SIMON KANAAN	2432	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *5/21/2009*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-48* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-48* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. This action is responsive to communications: application, filed 01/18/2005; amendment filed 10/22/2008, RCE filed 5/21/2009.

Response to Arguments

2. Applicant's arguments filed 5/21/2009 have been fully considered but they are moot based on the new grounds of rejection as shown below.

Information Disclosure Statement

3. The information disclosure statement (IDS) submitted on has been acknowledged. The submission is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

Claim Rejections - 35 USC § 103

4. Claims 1-4, 19-23 and 37-39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Seheidt et al. (US 5,375,169) in view of Maurer (US 5,253,294).

With respect to claim 1, Seheidt et al. teaches that an apparatus for use by a first party for key management for secure communication with a second party, said key management being to provide at each party, simultaneously remotely, identical keys for said secure communication without transferring said keys over any communication link

(apparatus and method, for the secure communication of a message from a transmitting user to a receiving user using a split key scheme, col. 4, lines 29-32), the apparatus comprising: a datastream extractor, configured to extract a bitstream from data exchanged between said parties (the key components generated by the cryptographic engine is a pseudorandom sequence of bits of a particular length with an appended error detection field which mathematically calculated based on the pseudorandom sequence, col. 4, 36-41), but fails to teach a random selector.

However, Maurer teaches that a random selector configured with selection settings identical to those at said second party for selecting, from said bitstream, a series of bits in accordance with a randomization seeded by said data exchanged between said parties, said randomization being identical to a randomization carried out at said second party, thereby ensuring that said series of bits is identical at both parties, a key generator configured for separately generating at said first party a key for encryption/decryption based on said series of bits. thereby to separately generate a key at said first party which is identical to a key likewise generated at said second party based on said exchanged information, thus to manage key generation in a manner repeatable at said parties. –Maurer, figure 1, key index generator sends signal to two different parties which have their own randomizers which create identical keys. One party uses the key to encrypt and send the message. The second party receives the message and decrypts it with its own generated key.

It would have been obvious at the time the invention was made to a person having ordinary skill in the art to modify Seheidt et al. with random selector and key

generator of Maurer to prevent the need for transferring keys and secure communication of a message from a transmitting user to a receiving user.

With respect to claim 2, Maurer teaches that the random selector being operable to use results of said randomization as addresses to point to bits in said datastream – Maurer, figure 1, key index generator sends signal to two different parties which have their own randomizers which create identical keys. One party uses the key to encrypt and send the message. The second party receives the message and decrypts it with its own generated key.

With respect to claim 3, Seheidt et al. teaches that said key generator operable to generate a new key after a predetermined number of message bits have been exchanged between said parties (new keys are generated every time a new message is communicated between parties, col. 8, lines 31-33). It would have been obvious at the time the invention was made to a person having ordinary skill in the art to modify the above references to prevent compromise of the key.

With respect to claim 4, Seheidt et al. teaches that said predetermined number of message bits being substantially equal to a length in bits of said key (alternatively, the key may remain the same as long as the same parties are in communication, col. 8, lines 33-34).

With respect to claim 19, Seheidt et al. teaches that said system being operable to provide key management for a symmetric cryptography algorithm (An alternative to the public key system is a private key system known as a symmetric key system which is a cryptographic system using the same key for both encryption and decryption. This key is transmitted from the sender to the receiver over a secure channel in parallel with the encrypted message, col. 3, lines 38-44).

With respect to claim 20, Seheidt et al. teaches that being constructed modularwise such that said cryptography algorithm is exchangeable (In addition to the protection of the keys themselves, selecting the proper key sequence and increasing the frequency with which the key sequence is changed can enhance the security of this type of protection, col. 2, lines 2-6).

Claim 21 differs from claim 1 only in that claim 1 is an apparatus claim whereas, claim 21 is a system claim. Thus, claim 21 is analyzed as previously discussed with respect to claim 1 above.

With respect to claim 22, Seheidt et al. teaches that said primary bitstream is obtainable as a stream of bits from a data communication process between said two parties (The key component is a pseudorandom sequence of bits with an appended error detection field which is mathematically calculated based on the pseudorandom sequence, abstract).

With respect to claim 23, Seheidt et al. teaches that teaches that said bits in said primary bitstream are separately identifiable by an address, and wherein said selector is operable to select said bits by random selection of addresses (The pseudorandom sequence is generated using known pseudorandom sequence generating means within the cryptographic engine 24, for example, through the use of serial shift registers having selected outputs modulo-2 added and fed forward, col. 6, lines 29-34)

Claim 37 differs from claim 1 only in that claim 1 is an apparatus claim whereas, claim 37 is a method claim. Thus, claim 37 is analyzed as previously discussed with respect to claim 1 above.

With respect to claim 38, Seheidt et al. teaches that said primary data source is obtainable as a stream of bits from a communication process between said two parties (The key component is a pseudorandom sequence of bits with an appended error detection field which is mathematically calculated based on the pseudorandom sequence, Abstract).

With respect to claim 39, Seheidt et al. teaches that said primary data source comprises a stream of data bits divisible into data units and comprising selecting at random from the data bits of each data unit (The pseudorandom sequence is generated using known pseudorandom sequence generating means within the cryptographic

engine 24, for example, through the use of serial shift registers having selected outputs modulo-2 added and fed forward col.6, lines 29-35).

5. Claims 5-18, 24-36 and 40-48 are rejected under 35 U.S.C. 103(a) as being unpatentable over Seheidt et al. (US 5,375,169) in view of Maurer (US 5,253,294) as applied to claim 1 above, and further in view of Khamharn et al. (5,375,169).

With respect to claim 5, Seheidt et al. and Maurer don't teach that a control messager for sending control messages to said remote party, thereby to indicate to said remote party a state of said apparatus to enable said remote party to determine whether said remote party is synchronized therewith to generate an identical key. However, Khamharn et al. teaches that transmitting at least a first message from the transmitter to the receiver; and, in response to the receiver receiving the first message, the receiver detecting the absence of synchronization between the transmitter and the receiver and performing a resynchronization procedure to restore synchronization between the transmitter and the receiver, see abstract. It would have been obvious at the time the invention was made to a person having ordinary skill in the art to modify the above references with Khamharn et al. to perform and restore synchronization between the transmitter and the receiver.

With respect to claim 6, Khamharn et al. teaches that a synchronized state determiner, for determining from control messages received from a remote party

whether said apparatus is synchronized therewith to generate an identical key (The value stored in NSQN 66 is compared to SQN2 42 to determine what level of resynchronization may be required. Subsequent to a successful message 20 authentication, memory location SQN2 42 is updated to contain the value of SQN1 28 stored in NSQN 66, col. 5, lines 27-33).

With respect to claim 7, Khamharn et al. teaches that a resynchronizer, associated with said synchronous state determiner, said resynchronizer having a resynchronization random selector for selecting, from a part of said bitstream previously used by said random selector, a series of bits in accordance with a randomization seeded by said data exchanged between said parties (the random initial state is used as starting point, col. 3, lines 33-34), in the event of determination of synchronization loss, thereby to regain synchronization (Once synchronization is lost, the system does not respond and appears inoperative. Resynchronization is required to restore the system operation to normal, col. 1, lines 19-22).

With respect to claim 8, Khamharn et al. teaches that said series of bits is a series of bits previously used by said random selector (the random initial state is used as starting point, col. 3, lines 33-34).

With respect to claim 9, Khamharn et al. teaches that said control messager is operatively connected to said synchronous state determiner, thereby to include within

said control messages a determination of synchronization loss (transmitting at least a first message from the transmitter to the receiver; and, in response to the receiver receiving the first message, the receiver detecting the absence of synchronization between the transmitter and the receiver and performing a resynchronization procedure to restore synchronization between the transmitter and the receiver, abstract).

With respect to claim 10, Khamharn et al. teaches that said control messager is operatively connected with said resynchronizer, to control said resynchronizer to carry out said selection in the event of receipt of a message from said remote party that said remote party has lost synchronization (A first resynchronization process occurs within synchronization window 44, a resynchronization area whereby, subsequent to a first message 20 reception, SQN1 28 received is greater than SQN2 42 by not more than K increments, col. 4, lines 17-21).

With respect to claim 11, Khamharn et al. teaches that said data communication being arranged in cycles, said part of said bitstream being exchangeable in each cycle (Current systems require a manual sequence of operations for restoring synchronization, such as depressing lock and unlock buttons for a predetermined period of time and waiting for a lock cycle feedback, col. 1, lines 22-26).

With respect to claim 12, Khamharn et al. teaches that said cycle being arranged into sub-units, each said cycle having an exchange point at its beginning for carrying out

said exchange (CRC 32 which is a cyclic redundancy check code to permit receiver 18 t validate the integrity of message transmission, col. 3, lines 48-49).

With respect to claim 13, Khamharn et al. teaches that said messager being usable to exchange control messages with said remote party to ensure that a same bitstream part is used for resynchronization at both said parties (Message structure 20 provides for system security by preventing the deception of receiver 18 by interception, col. 3, lines 50-51).

With respect to claim 14, Khamharn et al. teaches that said messager being usable to vary a control message in accordance with a sub-cycle current at a synchronization loss event, thereby to control said remote party to resynchroni-ze using a same bitstream part (It is when received SQN1 28 does not match an expected value based on SQN2 42 that synchronization between transmitter 12 and receiver 18 is considered lost and resynchronization must occur, col. 3, lines 13-16).

With respect to claim 15, Khamharn et al. teaches that operable to respond to messages sent by a remote party following said synchronization loss event, to revert to same said bitstream part as said message indicates that said remote party intends to use (In this case, receiver 18 will execute a resynchronization process dependent upon receiving and verifying a second and a third message 20 reception, col. 4, lines 44-47).

With respect to claim 16, Khamharn et al. teaches that circuitry for determining which of itself and said remote party is a transmitting party and being operable to control said synchronization when it is a transmitting party and to respond to control commands of said remote party when said remote party is said transmitting party (Transmitter 12 emits RF signals 16 in response to use activation of one or more buttons 14 associated with transmitter 12. Receiver 18 periodically checks for the presence of a transmission and performs the requested function only if the fields within message structure 20 (FIG. 2) are intended for that particular receiver and contains valid security information, col. 3, lines 1-7).

With respect to claim 17, Khamharn et al. teaches that said synchronized state determiner comprises: a calculation circuit for carrying out an irreversible calculation on any one of said bitstream, said randomization, said key and derivations thereof, and a comparator for comparing a result of said calculation with a result received from said remote party, thereby to determine whether said parties are in synchronization (an initial first sequence number value (SQN1) 28, a random initial state (not shown), and a cryptographic key (not shown), col. 3, lines 27-30).

With respect to claim 18, Khamharn et al. teaches that said irreversible calculation comprises a one-way function (a calculation using an algorithm to combine a cryptographic key with function code 24 and CRC 32, col. 3, lines 46-48).

With respect to claim 24, Khamharn et al. teaches that each selector comprises an address generator and each address generator is identically set (function code 24 which identifies the fuction being requested, col. 3, lines 40-41).

With respect to claim 25, Khamharn et al. teaches that a controller for exchanging control data between said parties to enable each party to determine that each selector is operating synchronously at each party (transmitting at least a first message from the transmitter to the receiver; and, in response to the receiver receiving the first message, the receiver detecting the absence of synchronization between the transmitter and the receiver and performing a resynchronization procedure to restore synchronization between the transmitter and the receiver, see abstract).

With respect to claim 26, Khamharn et al. teaches that redundancy check data, and a hash encoding result, of at least some of the bits from said derived bit source (a cryptographic key with function code 24 and CRC 32 which is a cyclic redundancy check code, col. 3, lines 47-48).

With respect to claim 27, Khamharn et al. teaches that redundancy check data, and a hash encoding result, of at least some of the bits of said randomization (a cryptographic key with function code 24 and CRC 32 which is a cyclic redundancy check code, col. 3, lines 47-48).

With respect to claim 28, Kahmharn et al. teaches that redundancy check data, and a hash encoding result, of at least some of the bits from said key (a cryptographic key with function code 24 and CRC 32 which is a cyclic redundancy check code, col. 3, lines 47-48).

With respect to claim 29, Khamharn et al. teaches that redundancy check data of at least some of said addresses, and a hash encoding result of at least some of said addresses (a cryptographic key with function code 24 and CRC 32 which is a cyclic redundancy check code, col. 3, lines 47-48).

With respect to claim 30, Khamharn et al. teaches that at each party a resynchronizer operable to determine from said control data that synchronization has been lost between the parties and to regain synchronization based on a predetermined earlier part of said derived bit source (It is when received SQN1 28 does not match an expected value based on SQN2 42 that synchronization between transmitter 12 and receiver 18 is considered lost and resynchronization must occur, col. 4, lines 13-16).

With respect to claim 31, Khamharn et al. teaches that at each party a resynchronizer operable to determine from control data exchanged between said parties that synchronization has been lost between said parties and to regain synchronization based on a predetermined earlier part of said derived bit source synchronization (A first resynchronization process occurs within synchronization window 44, a

resynchronization area whereby, subsequent to a first message 20 reception, SQN1 28 received is greater than SQN2 42 by not more than K increments, col. 4, lines 17-21).

With respect to claim 32, Khamharn et al. teaches that said data communication process being arranged in cycles, said predetermined earlier part being exchangeable in each cycle (Current systems require a manual sequence of operations for restoring synchronization, such as depressing lock and unlock buttons for a predetermined period of time and waiting for a lock cycle feedback, col. 1, lines 22-26).

With respect to claim 33, Khamharn et al. teaches that said cycles being arranged into sub-units, each said cycle having an exchange point at its beginning for carrying out said exchange of said predetermined earlier part of said derived bit source (CRC 32 which is a cyclic redundancy check code to permit receiver 18 t validate the integrity of message transmission, col. 3, lines 48-49).

With respect to claim 34, Khamharn et al. teaches that said controller being usable to include in said control messages, data to ensure that a predetermined earlier part of said derived bit source of a same cycle is used for resynchronization at both said parties (In this case, receiver 18 will execute a resynchronization process dependent upon receiving and verifying a second message 20 reception, Co. 4, lines 36-40)

With respect to claim 35, Khamharn et al. teaches that said controller being usable to vary a control message in accordance with a sub-cycle current at a synchronization loss event, thereby to control said remote party to resynchronize using same said predetermined earlier part of said derived bit source (It is when received SQN1 28 does not match an expected value based on SQN2 42 that synchronization between transmitter 12 and receiver 18 is considered lost and resynchronization must occur, col. 3, lines 13-16).

With respect to claim 36, Khamharn et al. teaches that operable to respond to messages sent by a remote party following said synchronization loss event, to revert to same said predetermined earlier part of said derived bit source as said message indicates that said remote party intends to use (In this case, receiver 18 will execute a resynchronization process dependent upon receiving and verifying a second and a third message 20 reception, col. 4, lines 44-47).

With respect to claim 40, Seheidt et al. teaches that said bits in said data units are separately identifiable by addresses, and comprising selecting said bits by using said randomizer as an address pointer (The pseudorandom sequence is generated using known pseudorandom sequence generating means within the cryptographic engine 24, for example, through the use of serial shift registers having selected outputs modulo-2 added and fed forward, col. 6, lines 29-34).

With respect to claim 41, Seheidt et al. teaches that selecting is carried out by using identically set pseudorandom data generation at each party, and using said derived data source as a seed for said pseudorandom data generation (The pseudorandom sequence is generated using known pseudorandom sequence generating means within the cryptographic engine 24, for example, through the use of serial shift registers having selected outputs modulo-2 added and fed forward, col. 6, lines 29-34).

With respect to claim 42, Khamharn et al. teaches that exchanging control data between said parties to enable each party to determine whether they are operating synchronously with said other party (transmitting at least a first message from the transmitter to the receiver; and, in response to the receiver receiving the first message, the receiver detecting the absence of synchronization between the transmitter and the receiver and performing a resynchronization procedure to restore synchronization between the transmitter and the receiver, see abstract).

With respect to claim 43, Khamharn et al. teaches that redundancy check data of at least some of said derived data source, and a hash encoding result of at least some of said derived data source (a cryptographic key with function code 24 and CRC 32 which is a cyclic redundancy check code, col. 3, lines 47-48).

With respect to claim 44, Khamharn et al. teaches that determining from said control data that synchronization has been lost between the parties and regaining synchronization based on a predetermined earlier part of said derived data source (It is when received SQN1 28 does not match an expected value based on SQN2 42 that synchronization between transmitter 12 and receiver 18 is considered lost and resynchronization must occur, col. 3, lines 13-16).

With respect to claim 45, Khamharn teaches that further comprising a step of exchanging said predetermined earlier part of said derived data source at predetermined intervals (sequence of operations for restoring synchronization, such as depressing lock and unlock buttons for a predetermined period of time and waiting for a lock cycle feedback, col. 1, lines 24-27).

With respect to claim 46, Khamharn teaches that determining a possibility of each party being at a different cycle at synchronization loss, and controlling said resynchronization to use a same predetermined earlier part of said derived data source at both parties (It is when received SQN1 28 does not match an expected value based on SQN2 42 that synchronization between transmitter 12 and receiver 18 is considered lost and resynchronization must occur, col. 3, lines 13-16).

With respect to claim 47, Khamharn teaches that further comprising creating in advance a future cycle's predetermined earlier part of said derived data source for

resynchronizing with a party that has already moved to such a cycle (resynchronization process occurs in resynchronization area 52 whereby, subsequent to a first message 20 reception, SQN1 28 received is grater than auto-resync window 48 yet less than SQN2 42, col. 4, lines 41-44).

With respect to claim 48, Seheidt et al. teaches that in use to provide key management for a symmetric cryptography algorithm (An alternative to the public key system is a private key system known as a symmetric key system which is a cryptographic system using the same key for both encryption and decryption. This key is transmitted from the sender to the receiver over a secure channel in parallel with the encrypted message, col. 3, lines 38-44).

Conclusion

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Simon Kanaan whose telephone number is (571) 270-3906. The examiner can normally be reached on Monday to Friday 8:30 AM to 5:00 PM.

If attempts to reach the above noted Examiner by telephone are unsuccessful, the Examiner's supervisor, Gilberto Barron, can be reached at the following telephone number: (571) 272-3799.

The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300. Information regarding the status of an application may be

obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/SIMON KANAAN/
Examiner, Art Unit 2432

/Gilberto Barron Jr./
Supervisory Patent Examiner, Art Unit 2432